

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

§

v.

§ CRIMINAL ACTION NO.

RENE QUIMBY (1)

§ 3:11-CR-018-B (01)

§

§

FACTUAL RÉSUMÉ

INDICTMENT: Count One: Fraud and Related Activity in Connection with Access Devices in violation 18 U.S.C. § 1029(a)(2);

Count Three: Aggravated Identity Theft in violation of 18 U.S.C. § 1028A.

**ELEMENTS OF
THE OFFENSE:**

Count One:

First: That Quimby knowingly used one or more unauthorized access devices;

Second: That by one or more uses during the one-year period beginning January 1, 2007, and ending December 31, 2007, Quimby obtained a thing or things, having an aggregate value of \$1000 or more;

Third: That Quimby acted with the intent to defraud; and

Fourth: That Quimby's conduct affected interstate commerce.

Count Three:

First: That Quimby knowingly possessed or used, without lawful authority, a means of identification that he knew belonged to another real person; and

Second: That Quimby possessed or used the means of identification of another real person during and in relation to committing fraud related activity in connection with access devices in violation 18 U.S.C. § 1029(a)(2), as charged in Count One of the Indictment.

STIPULATED FACTS

The Army and Air Force Exchange Service (“AAFES”) is a non-appropriated fund instrumentality of the United States government. It owns and operates roughly 3100 retail outlets called Post or Base Exchanges that reside on military installations, and are similar to any civilian retail outlet (such as Wal-Mart). AAFES also transacts retail commerce online at AAFES.com.

AAFES is a revenue-producing instrumentality that generates roughly ten billion dollars in revenue per year, mainly through the sale of merchandise and services to military personnel and their dependents. Net profits generated from this activity are primarily distributed to welfare funds, which are used for the collective benefit of military personnel and their dependents to provide for their morale, welfare, and recreation.

Rene Quimby installed on his computer various file-sharing programs (such as Etomi Pro, Frostwire, and Rocket) that allow computer users to share electronic files directly with each other using peer-to-peer networks. Quimby used these programs to

search for and download off of other users' computers files containing personally identifiable information, to include: names, dates of birth, social security numbers, addresses, phone numbers, bank account numbers, credit card numbers, and user names and passwords to various online accounts, as well as other means of identification.

Quimby used this information to make fraudulent online purchases.

On the peer-to-peer networks, Quimby found various military rosters that contained servicemembers' names, duty stations, name of command, dates of birth, rank, dates of rank, social security numbers, addresses, phone numbers, and spouse information. Quimby learned of the AAFES.com website when he downloaded a file that contained a servicemember's username and password for an AAFES account. He then learned that he could use servicemembers' social security numbers and dates of birth to log into the site. From there, Quimby used the online customer service chat feature and servicemembers' personal information to obtain their military STAR credit card numbers. Once he had their military STAR credit card numbers, he would order online numerous items, such as: computers, digital cameras, Apple iPods, and washer and dryers, and have them sent to various addresses in California where he would retrieve them. In particular, between January 1, 2007, and December 31, 2007, Quimby used the personally identifiable information for D.N., A.P., L.M., and S.H. to log into AAFES.com, obtain their military STAR credit card numbers, and then make thousands of dollars in purchases.

Quimby was able to download numerous images of peoples' checks from the peer-to-peer network, and use the account and routing numbers on the checks to make electronic payments to the military STAR credit cards so he could recharge them. At the time, AAFES would immediately credit the military STAR credit card account with the electronic check payment before the check or payment had actually cleared. Quimby was able to repeat this process, allowing him to "max-out" the military STAR credit cards over and over again. Quimby stopped making online purchases at AAFES.com after AAFES changed its policy preventing him from obtaining military STAR credit card numbers through the chat feature.

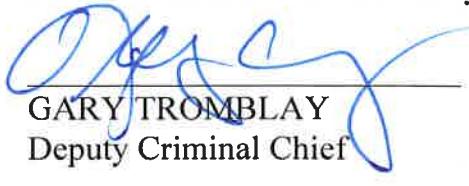
Quimby admits that he used more than one access device between January 1, 2007, and December 31, 2007. He admits he used them without authorization, he admits he used them with the intent to defraud, he admits he used them to obtain more than \$1000 in valuable merchandise over the internet, and he admits that his conduct affected interstate commerce. Finally, Quimby admits he used the means of identification of numerous people to commit fraud with access devices and he admits he knew these were real people.

SIGNED on this 9 day of May, 2011.


RENE QUIMBY
Defendant


CARLTON McLARTY
Attorney for Defendant


FRANK L. GATTO
Assistant United States Attorney


GARY TROMBLAY
Deputy Criminal Chief